

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-44 are pending in the application. Claims 1-2, 8, 11, 20-21, 22, 27 and 28 are amended by the present amendment. Claims 2, 8, 20, 22, 27 and 28 are amended to correct minor informalities noted in the outstanding Office Action. Support for amended independent Claims 1, 11 and 21 can be found at least at Fig. 7 and pp. 34-38 of the specification. No new matter is presented.

In the Office Action, Claims 8 and 20 are objected to because of minor informalities; Claims 2, 20, 22, 27 and 28 are rejected under 35 U.S.C. § 112, second paragraph; and Claims 1-44 are rejected under 35 U.S.C. § 102(b) as anticipated by Futamura et al. (U.S. Pub. 2002/0026582, herein Futamura).

In response to the objection to Claims 8 and 20, these claims are amended to correct the minor informalities noted in the Office Action. Accordingly, Applicants respectfully request that the objection to Claims 8 and 20 be withdrawn.

Claims 2, 20, 22, 27 and 28 are rejected under 35 U.S.C. § 112, second paragraph, as indefinite. In response to this rejection, Claims 2, 20, 22, 27 and 28 are each amended to correct the informalities noted in the Office Action.

More particularly, Claim 2 is amended to omit the term “in a related manner.” Claim 22 is amended to clarify that the “authentication information” has a term of validity and is related to a service provided by a first service providing section within the service providing section. Claim 27 is amended to remove the repetitive phrase “and an extended term of validity,” and Claims 22 and 28 are amended to remove the phrase “with respect.”

Accordingly, Applicants respectfully request that the rejection of Claims 2, 20, 22, 27 and 28 under 35 U.S.C. § 112, second paragraph, be withdrawn.

Claims 1-44 are rejected under 35 U.S.C. § 102(b) as anticipated by Futamura.

Applicants respectfully traverse this rejection as independent Claims 1, 11, 21, 22, 33 and 44 recite novel features clearly not taught or rendered obvious by the applied reference.

Independent Claim 1 relates to a service providing apparatus for providing services, comprising:

an authentication information managing section configured to manage authentication information ... having a term of validity;

an extension request accepting section configured to accept an extension request to extend the term of validity of the authentication information, ***judge whether the authentication information was created by the service providing apparatus by referring to an identifier included in the authentication information*** when the request to extend the term of validity of the authentication information is received, and judge whether the extension request was made within the term of validity of the authentication information if the ticket was created by the service providing apparatus; and

an authentication information updating section configured to extend the term of validity of the authentication information ***when the authentication information was created by the service providing apparatus*** and the extension request was made within the term of validity of the authentication information.

Independent Claims 11 and 21, while directed to alternative embodiments, are amended to recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of independent Claims 1, 11 and 21.

As described in an exemplary embodiment at Fig. 7 and pp. 34-38 of the specification, a service providing apparatus manages a ticket related to services, and the ticket has a term of validity. The service providing apparatus may receive an extension request to extend the term of validity of the ticket, and extend the term of validity of the ticket after determining that the ticket was created by the service providing apparatus and the request was made within the existing term of validity of the ticket.

Turning to the applied reference, Futamura describes an entity, such as a service provider (SP) and a user device (UC), which executes person authentication from an entity

that requests person authentication.¹ In rejecting the features of Claim 1, the Office Action relies on paragraphs [0658]-[0661] of Futamura.

This cited portion of Futamura, along with Fig. 85, describes a process used to update a person identification certificate (IDC) when it is determined that the "IDC expiration date" has been reached. The service provider 1002 checks, at scheduled intervals, the expiration date of the IDC stored in the service provider 1002. If it is detected that the IDC expiration date has been reached, the service provider 1002 requests the person identification certificate authority (IDA) 1001 to issue a new IDC. In accordance with the user ID, the IDA 1001 creates a new IDC in which a new expiration date is set using the user template information which has already been stored. The created IDC is transmitted to the service provider 1002 where it is then stored.

Thus, in Futamura, the IDCs are not managed by the service provider 1002, but are instead managed by the IDA 1001. Therefore, the IDC is not created by the service provider 1002 and the service provider 1002 does not *judge whether the authentication information was created by the service providing apparatus by referring to an identifier included in the authentication information* when the request to extend the term of validity of the authentication information is received," as recited in amended independent Claim 1. Moreover, Futamura fails to teach or suggest that either of the IDA 1001 or the service provider 1002 judge whether the IDC was created by either the IDA 1001 or the service provider 1002 when determining whether to issue a new IDC with a new expiration date.

Therefore, Futamura fails to teach or suggest a service providing apparatus for providing services that includes "an extension request accepting section configured to accept an extension request to extend the term of validity of the authentication information, *judge whether the authentication information was created by the service providing apparatus by*

¹ Futamura, Abstract.

referring to an identifier included in the authentication information when the request to extend the term of validity of the authentication information is received... and an authentication information updating section configured to extend the term of validity of the authentication information *when the authentication information was created by the service providing apparatus...*," as recited in amended independent Claim 1.

Accordingly, Applicants respectfully request that the rejection of Claims 1 (and the claims that depend therefrom) under 35 U.S.C. § 102 be withdrawn. For substantially similar reasons, it is also submitted that independent Claims 11 and 21 (and the claims that depend therefrom) patentably define over Futamura.

Independent Claim 22 recites, in part, a service providing apparatus, comprising:

a creating request sending section configured to send an authentication information creating request requesting creation of authentication information, the authentication information having a term of validity...

an extension request sending section configured to send an extension request requesting *extension of the term of validity of the authentication information*.

Independent Claims 33 and 44, while directed to alternative embodiments, recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of independent Claims 22, 33 and 44.

In rejecting the features of Claims 22, 33 and 44, the Office Action again relies on paragraphs [0658]-[0661] of Futamura. As discussed above, this cited portion of Futamura, along with Fig. 85, describes a process used to update a person identification certificate (IDC) when it is determined that the "IDC expiration date" has been reached. If it is detected that the IDC expiration date has been reached, the service provider 1002 requests the person identification certificate authority (IDA) 1001 to issue a new IDC. In accordance with the user ID, the IDA 1001 creates a new IDC in which a new expiration date is set using the user template information which has already been stored. The created IDC is transmitted to the service provider 1002 where it is then stored.

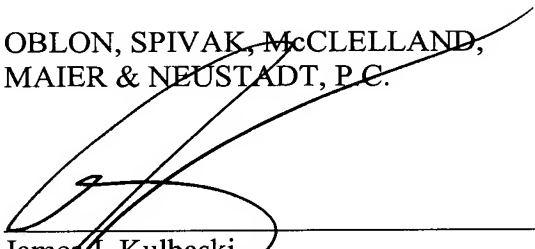
Therefore, Futamura describes creating a new IDC upon the expiration of a users previous IDC. Claim 22, in contrast, recites sending a request to extend the term of validity of “*the* authentication information” (i.e. already existing authentication information). The claimed configuration in which a term of validity of already existing (i.e. *the*) authentication information is extended, eases system resource burden by preventing the service providing apparatus from having to create new authentication information each time the authentication information expires, as is the case in Futamura.

Accordingly, for at least the reasons discussed above, Applicants respectfully request that the rejection of Claim 22 (and the claims that depend therefrom) under 35 U.S.C. § 103 be withdrawn. For substantially similar reasons, it is also submitted that independent Claims 33 and 44 (and the claims that depend therefrom) patentably define over Futamura.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1-44 is definite and patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



James J. Kulbaski
Attorney of Record
Registration No. 34,648

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)
I:\ATTY\ATH\PROSECUTION\24S\244714US\244714US AM DUE 9-10-08.DOC

Andrew T. Harry
Registration No. 56,959